

What is claimed is:

- 1 1. An architecture for confirming the identity of a message sender on a
2 remote services system, comprising:
3 a communications module operable to transmit a message;
4 a cryptographic module in said communication module for providing
5 encryption of a data stream in said message;
6 a mid-level manager operating in conjunction with said communications
7 module for controlling the flow of messages in said remote services
8 system and for verifying the identity of a sender by comparing first and
9 second data identities in said data stream.
- 1 2. The architecture according to claim 2, said first data identify
2 comprising data in a network software layer, said second data identity comprising
3 data in an application software layer.
- 1 3. The architecture according to claim 2, said cryptographic module
2 employing secure socket layer encryption.
- 1 4. The architecture according to claim 2, said mid-level manager
2 controlling data flow between a customer proxy and an applications server.
- 1 5. The architecture according to claim 4, wherein said mid-level manager
2 is a customer mid-level manager.
- 1 6. The architecture according to claim 4, wherein said mid-level manager
2 is an aggregation mid-level manager.
- 1 7. The architecture according to claim 2, wherein transmission of said
2 message is conditioned on HTTP.

1 8. The architecture according to claim 2, wherein transmission of said
2 message is conditioned on email protocol.

1 9. A method of confirming the identity of a message sender on a remote
2 services system, comprising:
3 obtaining a first identity related to a message, said first identity being obtained
4 from a first software layer in said remote services system;
5 obtaining a second identity related to the sender of a messages, said second
6 identity being obtained from a second software layer in said remote
7 services system; and
8 comparing said first identity with said second identity to verify the identity of
9 the sender of said message.

1 10. The method according to claim 9, said first software layer being the
2 network software layer, said second software layer being the application software
3 layer.

1 11. The method according to claim 10, further comprising encrypting said
2 message and said identities in an encryption module in said remote services system.

1 12. The method according to claim 11, said encryption of said data and
2 said identities being performed in accordance with secure socket layer protocol.

1 13. The method according to claim 12, said message being transmitted in
2 said system using HTTP protocol.

1 14. The method according to claim 12, said message being transmitted in
2 said system using email protocol.

1 15. A method of confirming the identity of a message sender on a remote
2 services system, comprising:

3 transmitting a message using a communications module of said remote
4 services system;

5 encrypting a data stream in said message using an encryption module in said
6 communications module; and

7 controlling the flow of said message in said remote services system using a
8 mid-level manager, said mid-level manager verifying the identity of a
9 sender by comparing first and second data identities in said data
10 stream.

1 16. The method according to claim 15, said first identity comprising
2 encrypted data in a network software layer of said remote services system, said
3 second identity comprising encrypted data in an application software layer of said
4 remote services system.

1 17. The method according to claim 15, said encryption module using
2 secure socket layer protocol to encrypt said data stream.

1 18. The method according to claim 17, said mid-level manager controlling
2 data flow between a customer proxy and an applications server.

1 19. The method according to claim 15, wherein said mid-level manager is
2 a customer mid-level manager.

1 20. The method according to claim 15, wherein said mid-level manager is
2 an aggregation mid-level manager.